CLAIMS

1. A method of connecting a mobile host to a remote network through an access network with a single user password, where the access network may be independent of the remote network in terms of no protocol conversation between authentication servers in the access network and the remote network, respectively, and a virtual single account (VSA) has been set up for a user to connect to the access network and then to the remote network, comprising the steps of:

generating a VSA password and decryption key from the single password received from the user;

decrypting at least one of a local access network authentication credential and a remote access authentication credential;

initiating a local access network connection; and

initiating a remote network access connection.

2. The method recited in Claim 1, further comprising the step of initiating a VSA configuration update process with a VSA server.

3. The method recited in Claim 2, wherein the VSA configuration update process comprises the steps of:

constructing a VSA information update request message;

sending the VSA information update request message to the VSA server; and

receiving a VSA information update response message from the VSA server.

4. The method recited in Claim 3, wherein the VSA information update request message contains an instruction authorizing the step of decrypting the remote network authentication credential prior to initiating the remote network access connection.

5. The method recited in Claim 1, further comprising the step of selecting a local access network from a current VSA access record.

6. The method recited in Claim 1, further comprising the step of generating the decryption key in response to a random sequence received from the user.

7. The method recited in Claim 1, wherein the VSA password is generated using the expression: VSA password = hash(VSA username || common password || VSA server || remote network ID), wherein the VSA username identifies the user to a VSA server, the common password is the single password from the user, and the remote network ID identifies the remote network serving as a home network for the mobile host.

8. The method recited in Claim 3, wherein the VSA update request message "Q" is derived from the expression: Q = VSA username || X || E_{K1} (Synchronization time || Request content), where X is a random sequence; and K1 is an encryption key calculated from hash (hash (VSA password) || X).

9. The method recited in Claim 8, wherein the VSA information update response message "A" is derived from the expression: A = Response Code || Y || E_{K2} (Synchronization time || Response content), wherein Y is a random

sequence, and K2 is an encryption key calculated from hash (hash (VSA password) || Y).

10. The method recited in Claim 1, further comprising the steps of selecting local access parameters and remote access parameters from a VSA access record.

11. A method of connecting a mobile host to a remote network through an access network with a single password, where the access network may be independent of the remote network in terms of no protocol conversation between authentication servers in the access network and the remote network, respectively, and a virtual single account (VSA) has been set up for a user to connect to the access network and then to the remote network, and a VSA server is deployed in the remote network, comprising the steps of:

receiving a VSA information update request message from the mobile host;

sending a VSA information update response message to the mobile host;

receiving an authentication credential for the remote network;

verifying the authentication credential; and

granting remote network access to the mobile host.

12. The method recited in Claim 11, wherein the VSA information update request message "Q" is derived from the expression: Q = VSA username || X || E_{K1} (Synchronization time || Request content), where X is a random sequence; and K1 is an encryption key calculated from hash (hash (VSA password) || X); and the VSA information update response message "A" is

derived from the expression: A = Response Code || Y || E_{K2} (Synchronization time || Response content), wherein Y is a random sequence, and K2 is an encryption key calculated from hash (hash (VSA password) || Y).

13. The method recited in Claim 11, wherein the VSA server contains a plurality of VSA management records, each management record including a user's VSA authentication credential.

14. The method recited in Claim 11, wherein the user's VSA authentication credential includes a VSA password generated from the single user password.

15. The method recited in Claim 14, wherein the VSA password is generated using the expression: VSA password = hash(VSA username || common password || VSA server || remote network ID), wherein the VSA username identifies a user to a VSA server, the common password is the single password from the user, and the remote network ID identifies the remote network serving as a home network for the mobile host.

16. The method recited in Claim 11, wherein the VSA server maintains access information for at least one local access network and at least one remote network.

17. The method recited in Claim 14, wherein the access information includes client information for mobile hosts, and management information for at least one additional VSA server.

18. The method recited in Claim 11, further comprising the step of a VSA server signaling a remote access gateway to verify the remote authentication credential.